Operationalizing a Zero Trust Architecture

August 2022

Introduction

The National Institute of Standards (NIST) first published the Risk Management Framework (RMF) in February of 2010 as a way to provide information security to operational systems. The US Government (USG) has since heavily relied upon the RMF and requires the application of the RMF to use a system operationally. While RMF has been modified and improved since its first publication, it still provides a basic or compliance-based set of criteria that improve the security posture of a mission critical system or application. However, the evolving threat and technology landscape have outpaced the applicability of the RMF to effectively secure against more advanced adversaries. In this paper, we introduce some alternative methodologies and frameworks for consideration to elevate the security posture of our systems.

The Emergence of Zero Trust

Information system security has traditionally relied upon a defensive principle that any system we are trying to protect from a threat should remain behind a fortified perimeter. In the mid-2010s, insider threat became one of the most damaging attacks for private and public organizations. Due to the fortified perimeter approach, users inside the perimeter boundary have abundant accesses that create additional risks, and once attackers establish valid credentials, they have free reign on several internal systems. This shift created a new security paradigm referred to as Zero Trust (ZT). ZT assumes the system/network perimeter could easily be compromised, and that all users should only be granted access to any system resource using a least-privilege approach. It also considers contextual information when providing such access.

In August 2020, NIST published Special Publication (SP) 800-207, which clearly defined the framework for a Zero Trust Architecture (ZTA). This publication coincided with the onset of the COVID-19 pandemic when a surge of remote users on untrusted devices were requesting access to enterprise resources. As a result, ZTA became a widely accepted framework for how to improve cybersecurity across organizations, but implementation and adoption has remained slow. In April 2021, the DoD published its Zero Trust Reference Architecture, a joint agency effort between the National Security Agency and the Defense Information Systems Agency, building upon the work NIST had produced with intent to progress the adoption of ZTA within the DoD. To bolster that, the Executive Office of the President published the Executive Order on Improving the Nation's Cybersecurity in May 2021, which required the USG to develop plans to implement ZTA. All of these developments seemed to drive the adoption of ZTA, but broad implementation of ZTA will require a paradigm shift in the decade-long approach to how the USG has historically and continues to secure and operate systems using the RMF.

Challenges of Pivoting To Zero Trust

Beyond the Executive Order which requires a "plan" to migrate to ZT, firm requirements are needed to implement ZT. In fact, the RMF and the security perimeter approach is still inherently required as part of the "Approval To Operate/Approval To Test" methodology. In addition, there is limited funding to change the historical way of doing business, and organizations lack incentives to do any more than is required. In a competitive market, meeting the minimum requirements is typically the most cost-effective approach.

Within the RMF, NIST's SP 800-53 provides a selection of controls based on the assessment of the impact of a system. HII's security engineers performed a preliminary mapping of ZT solutions to SP 800-53, and most fall under the Access Control family, which is only a subset of the controls required to fully implement RMF. This creates the perception that ZT only contributes a small component of an overall, existing solution, which drives up cost without a clear understanding of the actual benefit.

Implementing the DoD's ZT reference architecture also requires selecting ZT-enabled solutions and configuring them properly. Vendors have quickly latched on to the ZT philosophy, flooding the market with "Zero Trust enabled solutions" that comprise only a small piece of the overall puzzle and in many cases, provide overlapping capabilities. There is a lack of precedent and any authoritative guidance on which solutions should be applied and how they should be configured in order to properly implement a ZTA for a specific user-base, mission, or enterprise.

How We Move Forward

When the RMF was first released, it was met with confusion and skepticism, much like the current ZTA publications. Advancing ZT to fruition requires three key items: evidence, requirements, and funding. Proof of the ZT-enabled solution will turn the concept of increased security into religion as organizations will see the tangible benefit of moving beyond the "walled garden" approach and establishing ZT as the foundation for security. Establishing a clear set of requirements on how to implement ZT, backed with the authority to require that as a system security process, will leave few options for organizations to avoid implementation of ZTA. Finally, providing the adequate funding profiles to the organizations that must implement ZT, coupled with the requirements to do so and the confidence in the solution, will ensure that every organization has the resources they need to migrate to ZT.

In June and July of this year, NIST provided early implementation guidance for ZTA by publishing preliminary drafts of SP 1800-35A and 1800-35B. Further refinement of these guidance documents, along with organization-specific versions of these, will be required to understand how a ZTA implementation provides the best security. These should also address the end-state of a ZTA implementation, providing the knowledge and authority to organizations so they can determine when the implementation is "good enough" to stand up to an operational environment.

NIST and other USG organizations might also consider revising the RMF to include the ZT security framework and the processes to implement it. This approach will avoid conflicts with existing regulations, instructions, and law, such as the Federal Information Security Modernization Act. It also creates flexibility in how USG organizations apply security controls, while retaining the effectivity of a well-established risk management approach.

ZTA will accelerate the defensive posture of systems, forcing adversaries to change tactics and invest additional resources when attacking our systems. The USG clearly recognizes the added value of ZT and is on the road to operationalizing it, but there is still work to do before it becomes a routine process that

is instrumented across the enterprise. HII is piloting some of our own solutions to prove the worthiness of ZTA, leveraging our unique capabilities including the Big Data Platform (BDP), Threat-Based Cyber Security (TBCS), hardware/firmware validation, software methodologies (such as DevSecOps), and through our ongoing support to NIST, DISA, and NSA. Our goal is to provide evidence and guidance to our USG partners in order to accelerate adoption of ZT and improve the security of operational systems.